

Quantifying the Impact of Unavailability in Cyber-Physical Environments

Published in IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2014) part of the IEEE Symposium Series on Computational Intelligence (SSCI 2014), December 9-12, 2014
Orlando, FL

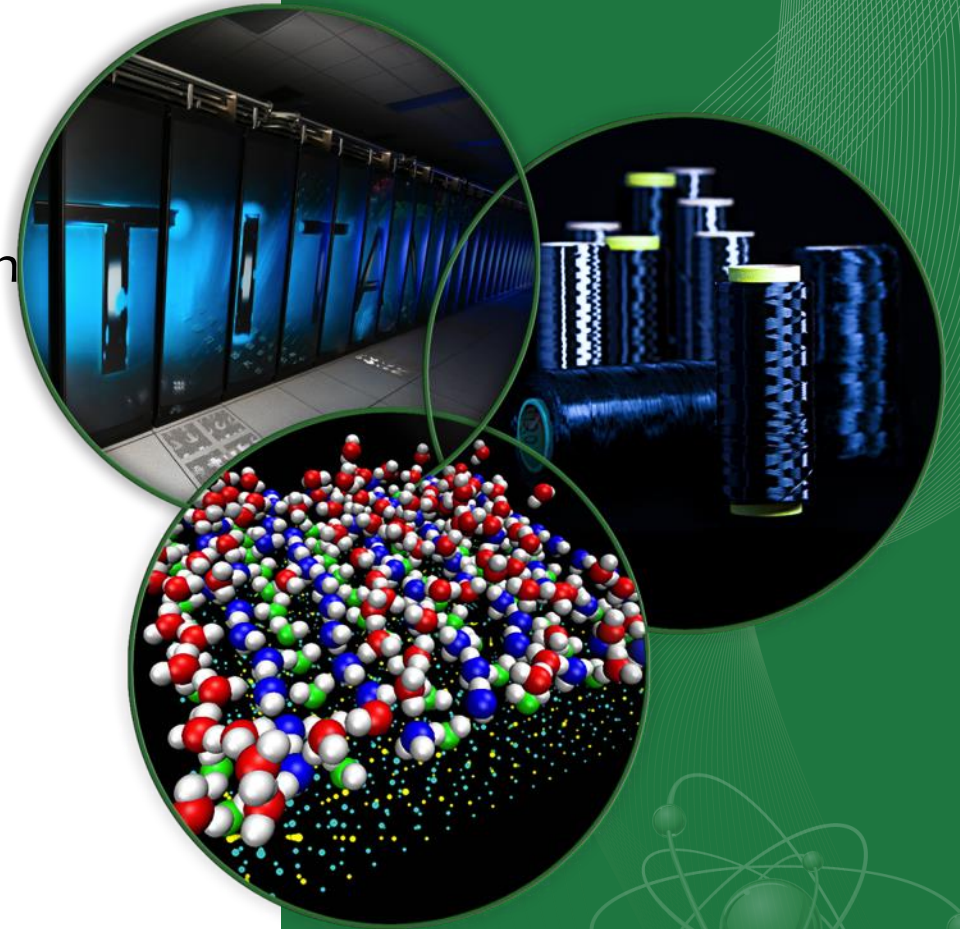
Resiliency Week August 20, 2015

Presenter:

Frederick T. Sheldon

Authors:

Anis Ben Aissa, Robert K. Abercrombie,
Frederick T. Sheldon, and Ali Mili



Agenda

- Introduction and motivation:
 - Cyber and information security fundamentals
 - Complex systems/risk management from perspective of a utility
- Foundations of Cyber Security Econometrics (CSE)
 - As a measure of Mean Failure Cost (MFC)
- Computational infrastructure for estimating the MFC using information about:
 - Security requirements,
 - System stakeholders and stakes,
 - System architecture, and
 - Threat configurations. }
- Application of CSE to STEG with regards to Availability:
 - Tunisian Company of Electricity and Gas (STEG: [Société Tunisienne de l'Electricité et du Gaz](#))
 - Econometric Availability (EA) calculated Using MFC, GAIN (gain/loss), and AVAIL (operational uptime)
- Conclusions and Future Directions

Attack surface all the reachable and exploitable vulnerabilities. *Software attack surface*: the complete profile of all functions in any code running in a given system that are available to an unauthenticated user.

Cyber and Information Security Fundamentals

Preliminary background rationale

The NIST Computer Security Handbook defines the term Computer Security as:

“The protection afforded to an automated information system to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources.”

Including: hardware, software, firmware, information/data, and telecommunications.

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information



Levels of Impact

Low

The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

High

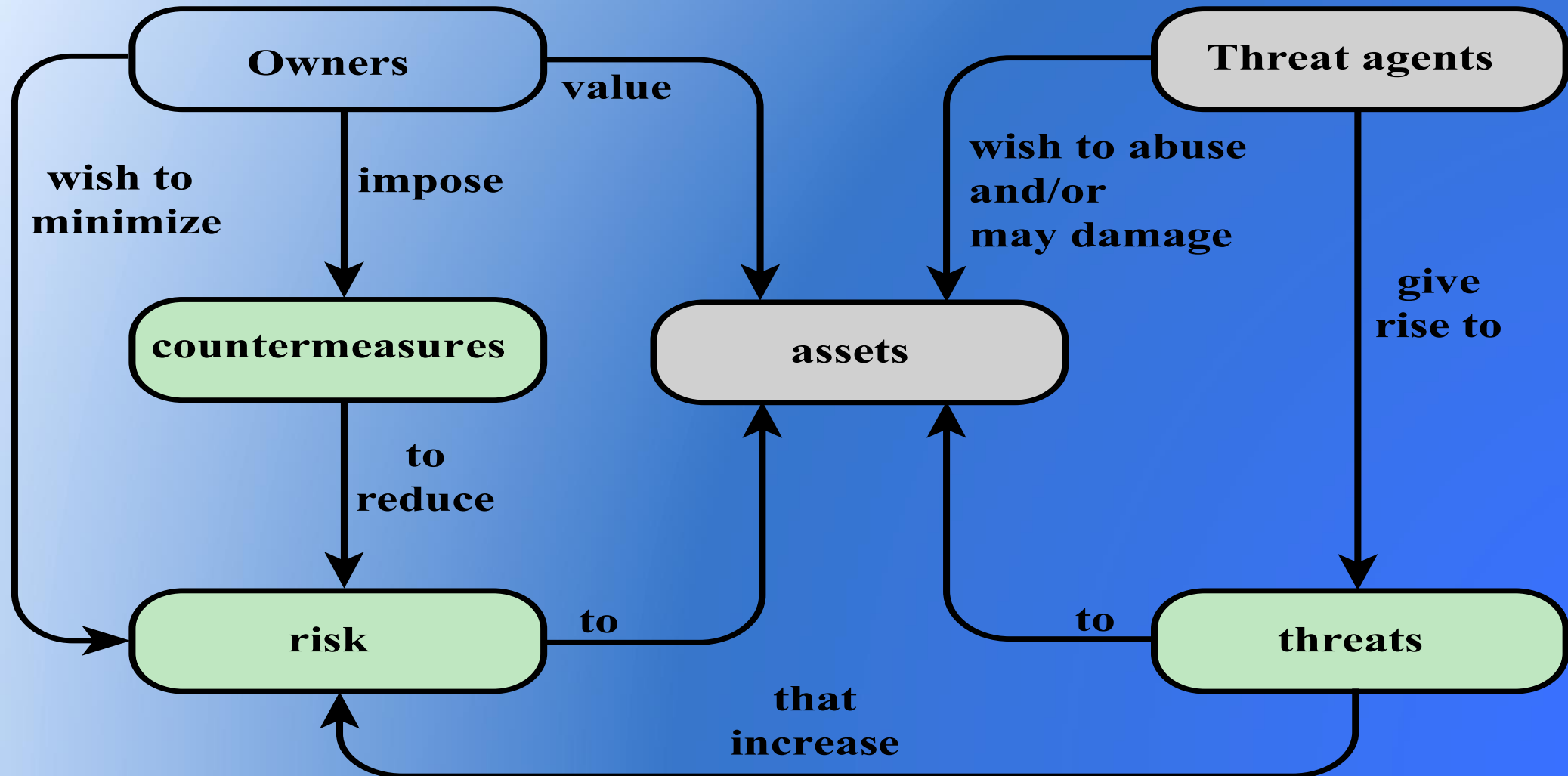
The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

COMPUTER SECURITY CHALLENGES

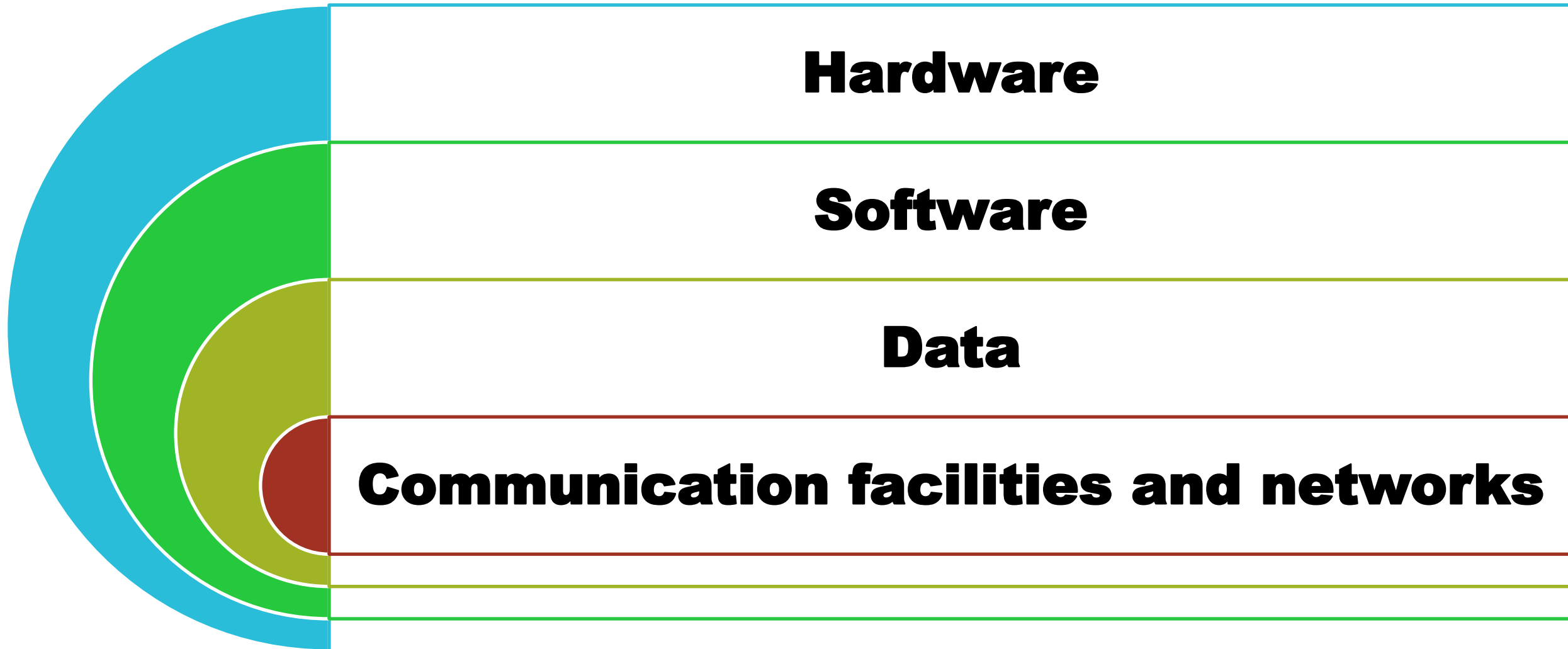
- Computer security is not as simple as it might first appear to the novice
- Potential unexpected attacks on the security features themselves *must be considered*
- Procedures used to provide security services are often counterintuitive ← **usability**
- Physical and logical placement needs to be determined
- Additional algorithms / protocols may be involved ← **new vulnerability introduced**
- Attackers only need to find a single weakness, the developer needs to find all weaknesses
- Users and system managers tend not see the benefits of security until a failure occurs
- Security requires regular and constant monitoring
- Is often an afterthought to be incorporated into a system after the design is complete
- Seen as an impediment to efficient and user-friendly operation

Key Security Concept:

Relationship among system resources (assets) that the owners wish to protect



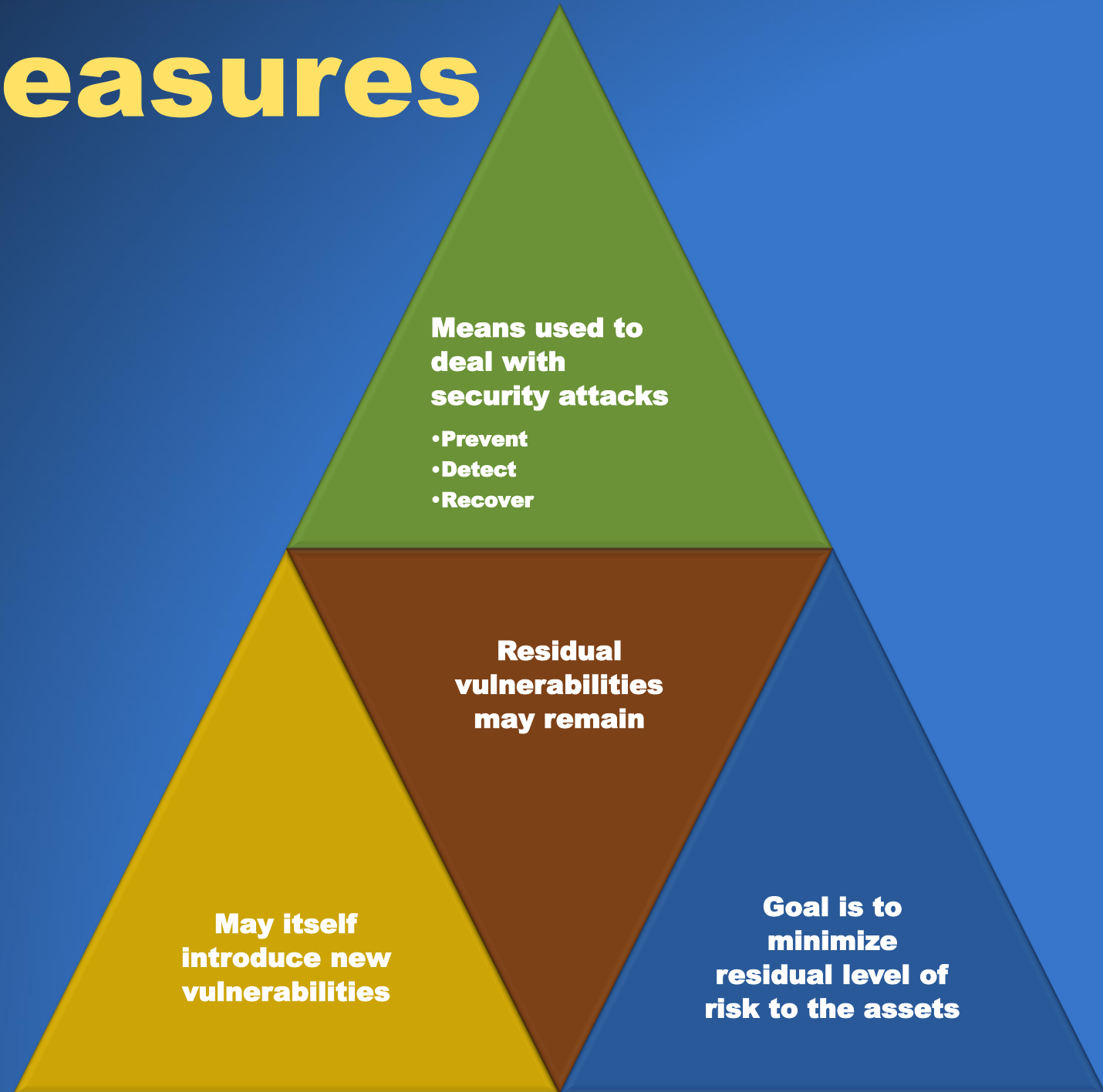
Assets of a Computer System



Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
 - Corrupted (loss of integrity)
 - Leaky (loss of confidentiality)
 - Unavailable or very slow (loss of availability)
- **Threats**
 - Capable of exploiting vulnerabilities
 - Represent potential security harm to an asset
- **Attacks (threats carried out)**
 - Passive – attempt to learn or make use of information from the system that does not affect system resources
 - Active – attempt to alter system resources or affect their operation
 - Insider – initiated by an entity inside the security perimeter
 - Outsider – initiated from outside the perimeter

Countermeasures





Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
 - Release of message contents
 - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
 - Replay
 - Masquerade
 - Modification of messages
 - Denial of service

Fundamental Security Design Principles

Economy of
mechanism

Fail-safe
defaults

Complete
mediation

Open design

Separation of
privilege

Least privilege

Least
common
mechanism

Psychological
acceptability

Isolation

Encapsulation

Modularity

Layering

Least
astonishment
(ergonomic)

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

Open ports on outward facing Web and other servers, and code listening on those ports

Services available on the inside of a firewall

Code that processes incoming data, email, XML, office docs, and industry-specific custom data exchange formats

Interfaces, SQL, and Web forms

An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Network protocol vulnerabilities, e.g., used for a DOS attack, disruption of communications links, and various intrusions

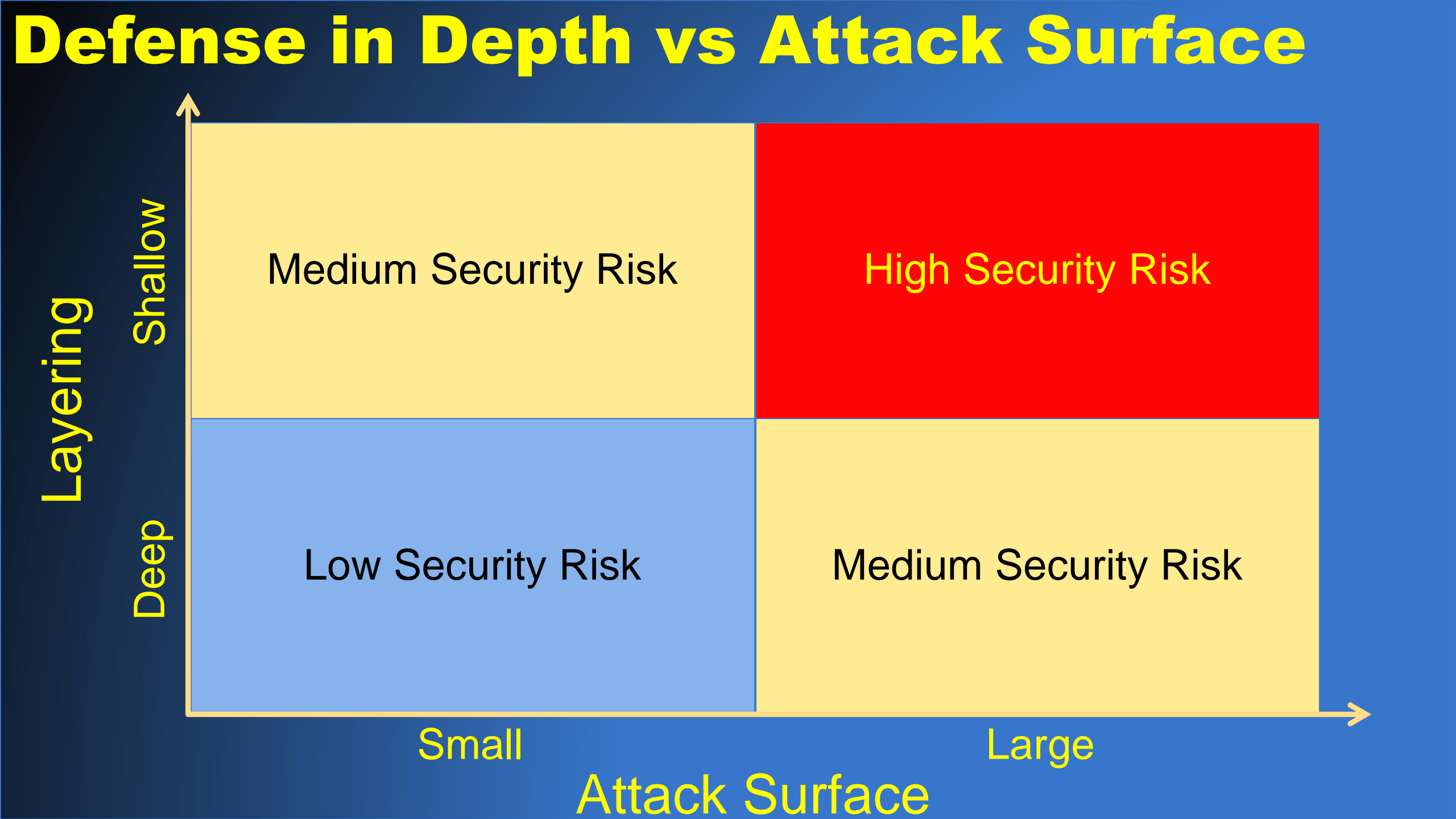
Software Attack Surface

Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

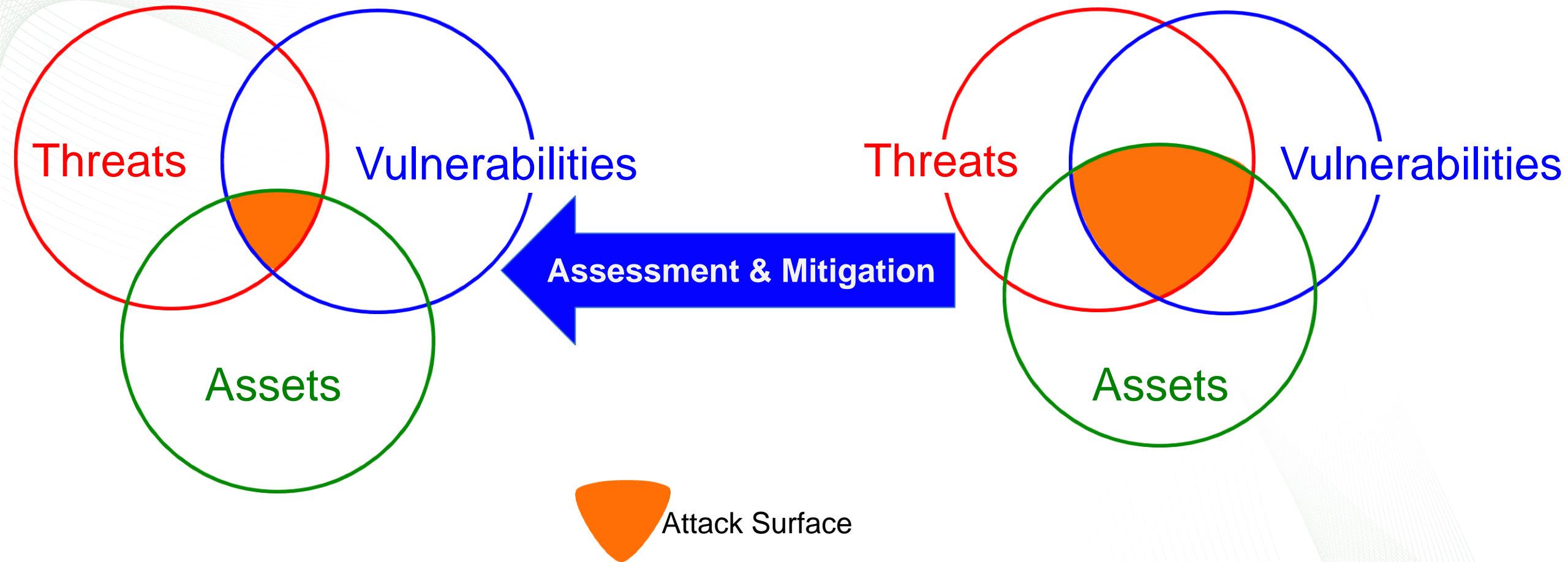
Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders



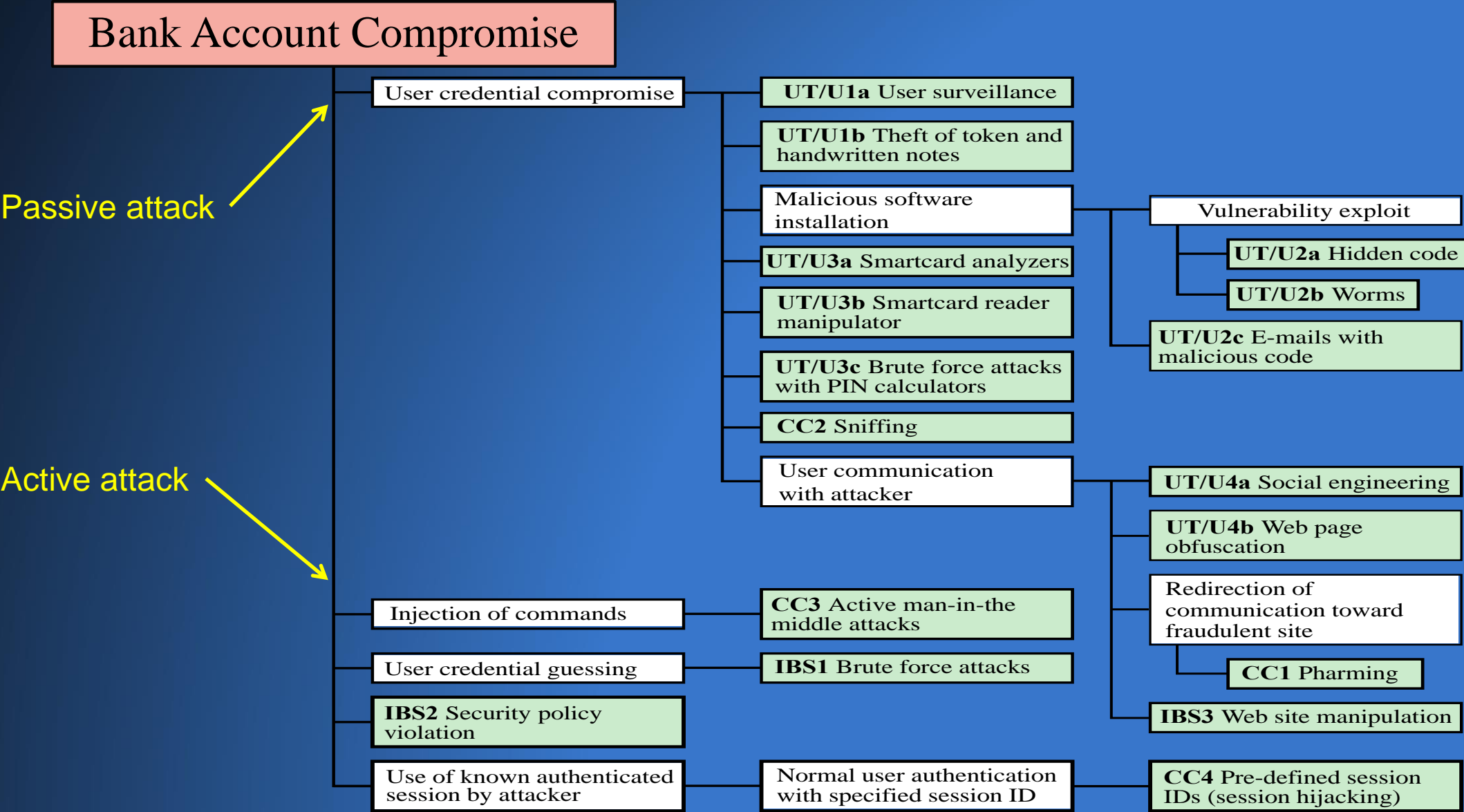
Attack Surface Conceptualized

Consist of the reachable and exploitable vulnerabilities in a system



A smaller attack surface can help to make your organization less exploitable and thereby reducing risk

Attack Tree: Internet Banking Authentication



Moving Target Paradigm ← Providing resilience through agility

- Research into Moving Target (MT) technologies will enable us to create, analyze, evaluate, and deploy mechanisms and strategies that are **diverse** and that **continually shift and change over time** to **increase complexity** and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and **increase system resiliency**.
- The characteristics of a MT system are dynamically altered in ways that are **manageable by the defender** yet make the **attack surface** appear **unpredictable to the attacker**.
- MT strategies aim to **substantially increase the cost of attacks** by deploying and operating networks and systems in a manner that makes them **less deterministic, less homogeneous, and less static**.

Every Computer Security Strategy Consists of:

Security Policy

Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Security Implementation

Involves four complementary courses of action:

- ✧ Prevention
- ✧ Detection
- ✧ Response
- ✧ Recovery

Assurance

The degree of confidence that the security measures, both technical and operational, work as intended to protect the system and information it processes and stores

Evaluation

Process of examining a computer product, system or network with respect to certain criteria (penetration testing, compliance and audit)

Developing a security policy

- A security manager needs to consider the following factors:
 - The value of the assets being protected
 - The vulnerabilities of the system
 - Potential threats and the likelihood of attacks

Summary

- Computer security concepts
 - Definition
 - Challenges
 - Model
- Threats, attacks, and assets
 - Threats and attacks
 - Threats and assets
- Security functional requirements
- Fundamental security design principles
 - Attack taxonomies include
 - Attack surfaces
 - Attack trees
 - Computer security strategy
 - Security policy
 - Security implementation
 - Assurance and evaluation

Cybernomics ← Cyberspace + Security + Economics

- Measurement methodology designed to assess the effectiveness of cybersecurity defenses, including the economic factors affecting individuals and organizations.
 - Involves market-based, legal, regulatory policy, or institutional interventions.
 - Includes *scientifically valid cost and risk analysis models and methods associated with sensible and enforceable notions of liability and care.*
 - Requires understanding the *motivations and vulnerabilities of both markets and humans*, and how these factors affect and interact with technical systems *within the ethos of cyberspace.*
 - Cybernomics should provide a common bottom line understanding of the risks and impacts to people and assets when combined with vulnerabilities and threats.

<http://cybernomics.ornl.gov>

Cybernomics premise

- Complex Systems
- Risk Management
- Good security metrics are required to make good decisions
 - Identifying a clear source (root cause) of the problem
 - Actionable for developing/deploying countermeasures
 - Common interpretation including simple and transparent computation
- The lack of sound and practical security metrics is severely hampering progress in the development of secure systems

Complex systems

- Composed of interconnected parts that as a whole exhibit one or more properties not obvious from the properties of the individual parts.

Risk Management

- Organizations typically use a risk management process to identify and mitigate risks to assure their organizational missions
 - For example, Department of Energy's [Cybersecurity RMP](https://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp)
 - energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp ([Released in 2012](#))
- Ideally documented, structured, and transparent process to identify critical resources, estimate threats and vulnerabilities that may intersect to cause harm (risks) to those resources.

Good security metrics are required to make good decisions about:

- How to design security countermeasures,
 - to choose between alternative security architectures,
 - to improve security during operations,
 - to effectively reduce the attack surface, and...
- are essential in understanding the effectiveness of investments aimed at improving security.

1940-1950s

1960's

1970's

1980's

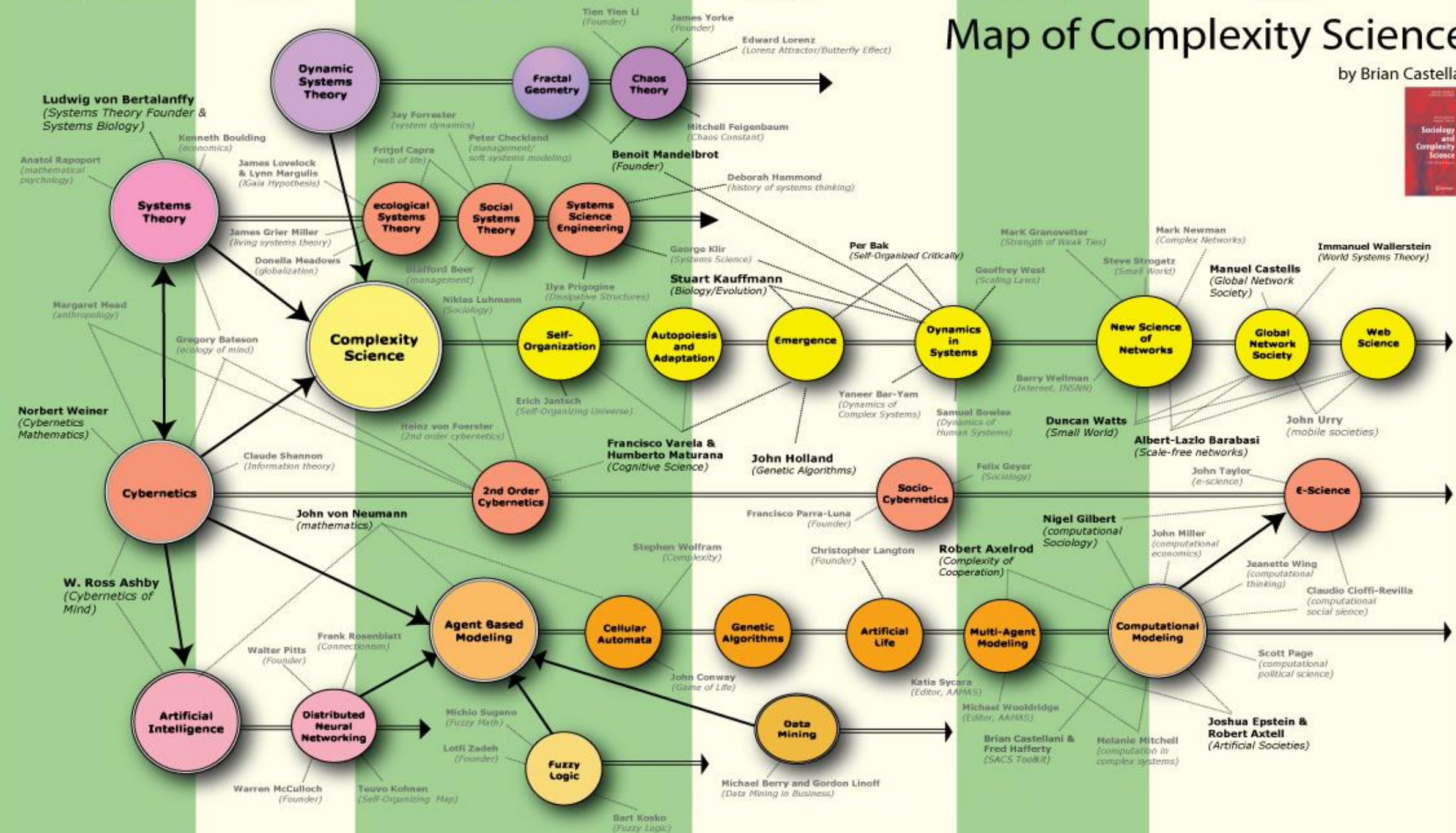
1990's

2000's

2010's

Map of Complexity Science

by Brian Castellani



Attributes of a “perfect” Metric ...

... must be combined with systematic data collection.

Gives clear evidence to root cause and necessary actions as metric changes

Actionable

People in the organization must recognize what the metric means

Common interpretation

The perfect metric

Accessible credible data

Transparent simple calculation

Data can be acquired with modest effort from a trusted source

How the metric is generated is shared and easy to understand

What is Needed for Disciplined Security Management?

- A logic
 - For specifying security requirements and verifying secure systems against such requirements.
- A computational model is necessary
 - For assessing system security by quantifying:
 - Costs, Risks, and
 - Measures/countermeasures and their potential impact;
 - For estimating ROI and for charging mitigation costs according to stakeholder benefit.
- Automated tools
 - That support security management according to the proposed models.



US008762188B2



(12) **United States Patent**
Abercrombie et al.

(10) **Patent No.:** US 8,762,188 B
(45) **Date of Patent:** Jun. 24, 2015

(54) **CYBERSPACE SECURITY SYSTEM**

(75) **Inventors:** Robert K. Abercrombie, Knoxville, TN (US); Frederick T. Sheldon, Knoxville, TN (US); Erik M. Ferragut, Oak Ridge, TN (US)

(73) **Assignee:** UT-Battelle, LLC, Oak Ridge, TN (US)

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 95 days.

(21) **Appl. No.:** 13/443,702

(22) **Filed:** Apr. 10, 2012

(65) **Prior Publication Data**

US 2012/0232679 A1 Sep. 13, 2012

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/421,933, filed on Apr. 10, 2009, now abandoned.

(60) Provisional application No. 61/052,556, filed on May 12, 2008.

(51) **Int. Cl.**
G06Q 10/00 (2012.01)
G06Q 10/04 (2012.01)

(52) **U.S. Cl.**
CPC **G06Q 10/04** (2013.01)
USPC **705/7.11; 705/7.36**

(58) **Field of Classification Search**
USPC 705/7.11–7.42
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,024,388 B2 4/2006 Stefek et al.
7,577,623 B2* 8/2009 Genty et al. 706/15
7,653,449 B2 1/2010 Hunter et al.
7,653,593 B2 1/2010 Zarikian et al.

7,672,866 B2 3/2010 Venkatraman et al.
8,312,549 B2 11/2012 Goldberg et al.
2003/0033542 A1 2/2003 Goseva-Popstojanova et al.
2003/0120652 A1* 6/2003 Tifft 70/
2004/0015728 A1 1/2004 Cole et al.
2004/0024606 A1 2/2004 Chukwu
2004/0103058 A1* 5/2004 Hamilton 705/
2004/0111220 A1 6/2004 Ochs et al.
2004/0230470 A1 11/2004 Svilar et al.
2005/0027379 A1* 2/2005 Dyk et al. 700/
2005/0050377 A1 3/2005 Chan et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP 63-191268 A 8/1988
WO WO 2004/070502 A2 8/2004

OTHER PUBLICATIONS

Frei, S., "Security Econometrics the Dynamics of (In) Security", Chapter 1, Sections 1.1-1.2, 2009, 23 pages.

(Continued)

Primary Examiner — Sujay Koneru

(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

A system evaluates reliability, performance and/or safety by automatically assessing the targeted system's requirements. A cost metric quantifies the impact of failures as a function of failure cost per unit of time. The metrics or measurements may render real-time (or near real-time) outcomes by initiating active response against one or more high ranked threats. The system may support or may be executed in many domains including physical domains, cyber security domains, cyber physical domains, infrastructure domains, etc. or any other domains that are subject to a threat or a loss.

22 Claims, 7 Drawing Sheets

DATE: January 5, 2015

TO: Robert K. Abercrombie and Frederick T. Sheldon

cc: S. S. Gleason, M. J. Paulus, File - RC

FROM: J. Caldwell 

SUBJECT: **Receipt of Invention Disclosure 201403444, DOE S-138,073, "Econometric Availability—A CSES Enhancement and Adaptation"**

Thank you for contributing to the outstanding technology being developed at Oak Ridge National Laboratory and for disclosing your recent invention for possible commercialization. Translating the scientific and technical accomplishments of the laboratory to the private sector is a key part of our mission and an important indicator of the impact we are making as a result of the nation's investment in ORNL.

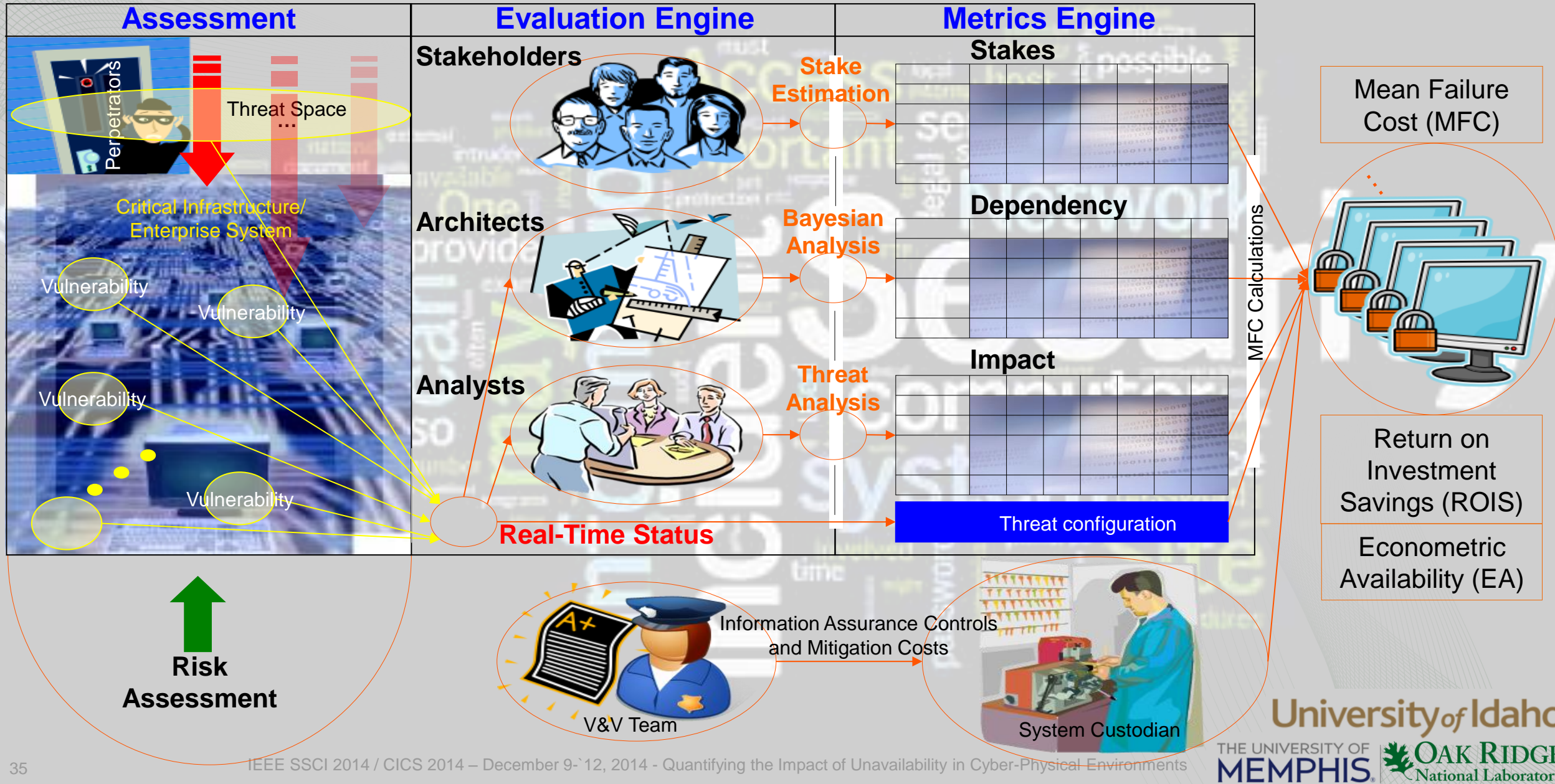
If it has not already been done, your commercialization manager, David Sims may schedule a meeting with you and the responsible patent agent to discuss. A copy of your invention disclosure is available upon request.

If you have any questions, please feel free to contact him at (865) 241-3808 or simsdl@ornl.gov.

Again, thank you for your invention disclosure. We look forward to working with you!

JTC:gts

Cyber Security Econometrics System Process



Stakes Matrix: Stakeholders vs. Requirements

- Premises necessary for MFC estimation:
 - A stakeholder may have different stakes in different requirements
 - A requirement may carry different stakes for different stakeholders
- Best represented with 2 dimensional matrix:
 - Rows: Stakeholders
 - Columns: Requirements
 - Entries: Stakes

		Requirements				
		R ₁	R ₂	R ₃	...	R _n
Stakeholders	S ₁					
	S ₂					
	S ₃					
	...				FC _{i,j}	
	S _m					

cost that stakeholder S_i would lose if the system failed to satisfy requirement R_j

Probability that the system fails to satisfy requirement R_j

$$MFC(S_i) = \sum_{R_j} FC_{i,j} \times P(R_j)$$

Dependency Matrix: Requirements vs. Components

		Components					
		C_1	C_2	C_3	...	C_k	C_{k+1}
Requirements	R_1						
	R_2						
	R_3						
	...				$\pi(R_i E_j)$		
	R_n						

- Links statistical correlations between component failures and requirements violations
- Assume that violations affect no more than one component at a time
- Let E_i , for $1 \leq i \leq k$, be the event: failure of component C_i
 - Event E_{k+1} : no component has failed

Probability of requirement violation R_i given component C_j fails

Probability of component C_j failing

Probability of requirement R_i violation

$$P(R_i) = \sum_{j=1}^{k+1} \pi(R_i|E_j) \times \pi(E_j)$$

Impact Matrix: Component Failure vs. Threats

		Threats					
		T_1	T_2	T_3	...	T_h	T_{h+1}
Components	C_1						
	C_2						
	C_3						
	...						
	C_k				$\pi(E_i V_j)$		
	C_{k+1}						

Probability of component C_i failing
given threat T_j materializes

Probability of
component C_j failing

$$\pi(E_i) = \sum_{j=1}^{h+1} \pi(E_i|V_j) \times \pi(V_j)$$

Probability of threat T_j
materializing

- To assess the likelihood a threat leads to a failed component:
 - Set of threats T_1, T_2, \dots, T_h
 - Events $V_1, V_2, \dots, V_h, V_{h+1}$
 - $V_i, 1 \leq i \leq h$: Threat i has materialized
 - V_{h+1} : No threat i has materialized
 - Assume that no more than one threat materializes at a time

Recall, E_j , for $1 \leq j \leq k$, is the event component C_j fails, and, event E_{k+1} : event no component has failed.

Summary of MFC Computations

$$MFC(S_i) = \sum_{R_j} FC_{i,j} \times P(R_j)$$

ST: Stakes Matrix (\$)

PR: Vector of requirement violation probabilities

$$MFC = ST \circ PR$$

$$P(R_i) = \sum_{j=1}^{k+1} \pi(R_i|E_j) \times \pi(E_j)$$

DP: Dependency Matrix

PE: Vector of component failure probabilities

$$PR = DP \circ PE$$

Probability
no dimension

$$\pi(E_i) = \sum_{j=1}^{h+1} \pi(E_i|V_j) \times \pi(V_j)$$

IM: Impact Matrix

PT: Vector of threat emergence probabilities

$$PE = IM \circ PT$$

Probability of an
event per unit time

\$/time unit

$$MFC = ST \circ DP \circ IM \circ PT$$

MFC: statistical mean of a random variable...

- Computed by taking into consideration a wide range of parameters,
 - Stakes that system stakeholders have in various cybersecurity requirements,
 - Statistical correlations between component failures and requirements violations,
 - Statistical dependencies between potential threats and component(s) failures (i.e., vulnerabilities), and
 - Statistical perpetrator models.
- These parameters are prone to change over time, therefore:
 - Each stakeholder should maintain a running estimate of their MFC in real-time.
- MFC has a wide *range of applications*, such as:
 - Triggering a cascade of counter-measures depending on the severity of the security violation,
 - Enhancing situational awareness for system stakeholders,
 - Planning dynamic risk mitigation strategies.

Quantifying Security: STEG Case Study

- A full-scale enterprise SCADA* system assessed within the domain of one utility
 - Tunisian Company of Electricity and Gas (STEG: [Société Tunisienne de l'Electricité et du Gaz](#)).
- [Analyzed service delivery and associated administrative controls](#) for electric power flow during a [one-year study period](#).
- All necessary data, including security requirements, stakeholders, components and the various threats (and actual attacks) were:
 - Collected by interviewing [STEG Managers/Subject Matter Experts](#).
- The information collected was [used to parameterize the MFC model](#).

*SCADA (Supervisory Control and Data Acquisition) systems serve as command and control for our electrical power grids, refineries, and other critical infrastructures.

IT/ICT Versus SCADA Security Requirements

- Availability, integrity, and confidentiality (listed in priority order in an IT context, as CIA) are the core requirements for cyber-physical security
- Typically requirements in SCADA systems focus on health, safety, environmental factors and operational availability/reliability
- Which result in reordering of priorities

Priority	Information Technology + Information and Communications Technology (IT/ICT)	SCADA
1.	Confidentiality	Availability
2.	Integrity	Integrity
3.	Availability	Confidentiality

Stakes (ST) Matrix for STEG SCADA System

- SCADA Stakeholder consolidated into 4 categories:
 - Maintenance personnel and operational personnel responsible for the maintenance and performance of all system operations,
 - System administrators responsible for the SCADA system administration functions,
 - Technical staff responsible for installing software and ancillary (non-admin type) materials/functions of the system,
 - Controllers of SCADA serves a vital role in maintaining safe and efficient systems operation (e.g., quality assurance/control).

Stakes Matrix (ST)		Security Requirements			
		Integrity	Availability	Confidentiality	Authenticity
Stakeholders	Maint. personnel	\$7,000	\$9,000	\$0	\$0
	System Admins	\$2,000	\$2,000	\$2,000	\$2,000
	Technical Staff	\$4,000	\$4,000	\$0	\$0
	Controllers	\$8,000	\$8,000	\$6,000	\$4,000

Dependency (DP) Matrix for STEG SCADA System

- DP Matrix was populated by *interviewing cyber security operations and system administrators* according to how much each component contributes to meeting each requirement as follows:
 - Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), Operating system (OS), Master Terminal Unit (MTU), I/O server (IOS), database server (DBS), Communication (C)

Dependency Matrix (DP)		Components							
		RTU	PLC	OS	MTU	IOS	DBS	C	No Failure
Security Requirements	Integrity	0.043	0.043	0.043	0.11	0.16	0.043	0.16	0.398
	Availability	0.043	0.043	0.043	0.11	0.16	0.043	0.16	0.398
	Confidentiality	0	0	0.08	0.08	0.08	0.08	0	0.68
	Authenticity	0	0	0.07	0.08	0.08	0.07	0	0.71

Impact (IM) Matrix for STEG SCADA System

- For the STEG SCADA system, the following threat categories were considered:
 - Unauthorized access (UAV), Malware (MV), Denial of service (DoS), Operating System vulnerability (OSV), Authentication (AV), Software vulnerability (SV), Human attacks (HAV), Hardware vulnerability (HV), and Communications vulnerability (CV)

Impact Matrix (IM)		Threats									
		UAV	MV	DoS	OSV	AV	SV	HAV	HV	CV	No Threats
Components	RTU	0	0	0.02	0.14	0	0.01	1x10 ⁻⁵	0.02	0.2	0.3499
	PLC	0	0	0.02	0.14	0	0.01	1x10 ⁻⁵	0.02	0.2	0.3499
	OS	0	0.01	0.02	0.1	0.001	0.2	0	0	0	0.669
	MTU	0.3	0.3	0.02	0.1	0.001	0.2	0	0.02	0.02	0.039
	IOS	0.3	0.02	0.02	0.02	0.001	0.2	0	0.02	0.02	0.399
	DBS	0.3	0.02	0.02	0.02	0.001	0.2	0	0.02	0.02	0.399
	C	0	0.01	0.02	0.01	0	0.01	0	0	0.5	0.45
	No Failure	0.1	0.64	0.86	0.47	0.996	0.17	0.99998	0.9	0.04	1

Threat Vector (PT) for STEG SCADA System

- A SCADA system can be attacked by a large number of threats. The following threat probability/hour were considered:

Threats	Probability/ hour
Unauthorized access (UAV)	0.0042
Malware (MV)	0.004
Denial of service (DoS)	0.0025
Operating System vulnerability (OSV)	0.003
Authentication (AV)	0.007
Software vulnerabilities (SV)	0.004
Human attacks (HAV)	1×10^{-5}
Hardware vulnerabilities (HV)	0.0007
Communications vulnerabilities (CV)	0.003
No Threats	0.97159

MFC as a Measure of Availability

- We adopt the following calculation that satisfies a global perspective for the STEG SCADA system. $AVAIL_{Op}$ is the operational availability,... the ratio of the system uptime and total time:

$$AVAIL_{Op} = Uptime / Operating Cycle$$

- Where, operating cycle is the overall period of operation under consideration and
 - Uptime is total time the system was actually functioning and available.
- We assume:
 - Independence with respect stakeholders,
 - Independence of the components, that have failed to ensure availability, and
 - Independence of threats, the root cause of security violations.

MFC as a Measure of Availability (cont.)

- Computational model used to assign cost (to affected stakeholders) of a security violation, or any such failure, for the *system under study*.
- Here, MFC describes a single attribute of dependability, namely the MFC of availability.
- We simply specify $AVAIL_{op}$ as a column vector (ST becomes ST'), and as a row vector (DP becomes DP').
- Thus, MFC has the same definition and has the following formula:

$$MFC = ST' \circ DP' \circ IM \circ PT$$

where, ST' is $n \times 1$; DP' is $1 \times h$; IM is $h \times p$; and PT is $p \times 1$.

MFC Accounting for Unavailability

- A **vector** of MFCs assessed using an updated Stakes Matrix (ST'), updated Dependency Matrix (DP'), the original Impact Matrix (IM) and the original Probability Threat (PT) vector for each class of stakeholder.
Initial MFC: \$25,129; Unavailability MFC: \$13,321

Stakeholder	Initial MFC (\$/hour)	MFC Accounting only for Unavailability (\$/hour)
Maintenance Personnel	\$6,437	\$5,220
System Administration	\$3,735	\$1,153
Technical Staff	\$3,218	\$2,316
Controllers	\$11,739	\$4,632

Emphasis on Availability ← Gain/Loss

- Redefining availability in value-oriented terms, we consider 3 factors:
 1. AVAIL: Defined earlier as the ratio of the system uptime and total time.
 2. The gain, per unit of time, is realized by stakeholder S from the system being operational; we denote this by $G(S)$. For the STEG utility, we let S be the company, then $G(S)$ represents the average revenue stream per unit of operational time.
 - The $G(S_i)$ for $1 \leq i \leq 4$ (column labeled “Gain”) was provided as data from interviews made with the STEG SMEs.
 3. The loss, per unit of time, is incurred by stakeholder S_i from the system being down; denoted $MFC(S_i)$.
 - For the STEG utility, S is the company, thus $MFC(S_i)$ represents lost business, productivity & customer loyalty due to downtime.

Definition of Econometric Availability (EA)

- AVAIL: Operational availability defined as ratio of the system uptime and total time.
 - **STEG year long study**: the operating cycle (mean time between failures [MTBF]) was 182.5 hrs.
 - **STEG historical records during one-year period**: maintenance teams required, on average, 3 hrs to repair system (MTTR) including both administrative and logistic downtime. Applying the formula gives operational availability AVAIL:
 - 98.38% (182.5 hrs/(182.5 hrs + 3 hrs))*.
- Therefore, using this concept of AVAIL and MFC, we define a value-oriented version of AVAIL namely, Econometric Availability (EA) represented by the following:

$$EA(S_i) = ((AVAIL \times G(S_i)) - ((1 - AVAIL) \times MFC(S_i)))$$

*Actual AVAIL ~ 98.4% from historical records; Notional AVAIL used later: 93%, 90%, 75%

Econometric Availability Using MFC, GAIN, and AVAIL

- Stakeholders & SMEs agreed, the classical formula of availability is inadequate to determine if the system is profitable or not. $AVAIL_{Op}$, operational availability, has a value in $[0, 1]$:
 - $AVAIL = 1$: percentage of availability of the system is 100% (high level of availability).
 - $AVAIL = 0$: system is unavailable (unacceptable).
 - $0 < AVAIL < 1$: system not guaranteed to be available.
- In all 3 cases the value of AVAIL does not provide a definitive understanding of system profitability. Thus, to make *availability* more useful in value-oriented terms, we used the EA formulation above.

Stakeholder S_i	MFC Adjusted (\$/hr)	Gain (S_i) (\$/hr)	EA (\$/hr) AVAIL = 98.4%	EA (\$/hr) AVAIL = 93%	EA (\$/hr) AVAIL = 90%	EA (\$/hr) AVAIL = 75%
Maintenance Per.	\$5,220	\$340	\$250	-\$49	-\$216	-\$1,048
System Admins	\$1,153	\$197	\$175	\$103	\$62	-\$140
Technical Staff	\$2,316	\$170	\$130	-\$4	-\$49	-\$451
Controllers	\$4,632	\$620	\$535	\$252	\$95	-\$693

$$EA(S_i) = ((AVAIL \times G(S_i)) - ((1 - AVAIL) \times MFC(S_i)))$$

Quantifying the Impact of Unavailability: EA

- The new formula, Econometric Availability (EA) can be used to evaluate the availability of a system in terms of the gain/loss (\$/hr of ops) that each stakeholder stands to gain/lose as a result of unavailability.

There are four cases:

- $EA(S_i) = G(S_i)$: System is available with an average of 100% gain per unit of time
- $EA(S_i) = -MFC(S_i)$: System is unavailable: MFC(S) is average loss per unit of time
- $(1-AVAIL) \times MFC(S_i) < EA(S_i) < 0$: System is available but not profitable
- $AVAIL \times G(S_i) > EA(S_i) > 0$: System is available and profitable

$$EA(S_i) = ((AVAIL \times G(S_i)) - ((1-AVAIL) \times MFC(S_i)))$$

Conclusions

- STEG SCADA system: *all selected stakeholders are profitable.* However, this will not always be true.
- Had we had chosen other stakeholders,...
 - whose MFC and Gain parameters were marginal, and whose AVAIL was approximately $\geq 15\%$ less, then:
 - the values under the 93%, 90% or 75% column headings would show a situation where all the stakeholders become unprofitable.
- SCADA systems used in critical infrastructures are characterized by
 - Interdependencies (physical, cyber, geographic, and logical) and
 - Complexity (collections of interacting components).
 - Abstract away other requirements to achieve the right level of complexity

Conclusions and Future Direction

- The critical nature and high cost of failures causing unavailability make EA an important metric to ascertain.
- The classical formula based on time between failure and time to recovery does not adequately convey the stakes (i.e., profitability).
- This approach can be used to focus on other important requirements
- *Plan to experiment with the AVAIL parameter to investigate the sensitivity of the EA formulation*
 - *e.g., assume that MFC and the Gain are fixed by the characteristics of the system.*
- *Develop case studies using Google Docs forms to systematically capture data in a more consistent/structured fashion*

University of Idaho

875 Perimeter Drive MS 1010
Moscow, ID 83844-1010

Frederick Sheldon

Professor and Chair

Computer Science Department

College of Engineering

PHONE : 208-885-6501

CELL : +01-865-621-8908

FAX : 208-885-9052

EMAIL : sheldon@uidaho.edu

WEB : www.uidaho.edu/engr/cs